Security Education

Introduction

Each military member is required to receive security education training upon entry into the service. This lesson fulfills that requirement. It offers information about our operations security program (OPSEC), to include communications security (COMSEC), emission security (EMSEC), computer security (COMPUSEC), and protection of the President.

Study Assignment

Read the information section of this lesson.

Lesson Objective: Know the importance of Air Force security.

Samples of Behavior:

1. Define OPSEC, COMSEC, EMSEC, and COMPUSEC.
2. State the types of security classifications under classified and unclassified information.
3. Identify your responsibilities under COMPUSEC.
4. State your responsibility regarding protection of the President.

Information

Operations Security (OPSEC)

Operations Security (OPSEC) is the process of denying adversaries information about friendly capabilities and intentions. This process is accomplished by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities. OPSEC applies at all levels of command. Individuals are responsible for complying with established security practices for protecting classified and unclassified information, which they've been exposed to.

<u>Classified</u> information is official information, which, in the interest of our national security, requires protection against unauthorized disclosure. Only those individuals, who possess the proper security clearance, have a need to know, and present proper identification can be granted access to classified information. Proper security clearance means the individual must have a clearance equal to the classification level of the information.

A person who doesn't meet these requirements can't have access to classified information. A security incident occurs if someone who doesn't meet all these requirements accidentally sees, or has access to classified information.

There are four types of security incidents: compromise, probable compromise, inadvertent access, and security deviation.

a. **COMPROMISE** - Compromise is defined as the known or suspected exposure of classified information or material to an unauthorized person. The compromise of classified information presents a threat to our national security. The seriousness of that threat must be determined, and appropriate measures must be taken to minimize the adverse effects of such a compromise. Action must be taken to regain custody of the material and to identify and correct the cause of the compromise.

b. **PROBABLE COMPROMISE** - An incident in which a reasonable presumption exists that an unauthorized person had or has access to classified information.

c. **INADVERTENT ACCESS -** An incident in which a person had or has access to classified information to which the individual was or isn't authorized, but was or is the subject of a favorable personnel security investigation permitting the granting of an interim or final security clearance to the level category of classified information involved.

d. **SECURITY DEVIATION** - An incident that involves the misuse or improper handling of classified material, but doesn't fall into the previous three categories.

The most critical part of the security system is the act of determining and assigning a security classification. The key in this determination is whether the national defense risks are grave enough to classify and withhold the information from unauthorized persons. There are three security classifications for <u>classified</u> information. They are:

a. **Top Secret.** National security information or material that requires the <u>highest</u> degree of protection and the unauthorized disclosure of which could reasonably be expected to cause **exceptionally grave damage** to national security.

b. **Secret.** National security information or material that requires a <u>substantial</u> degree of protection and the unauthorized disclosure of which could reasonably be expected to cause **serious damage** to national security.

c. **Confidential.** National security information or material that requires protection and the unauthorized disclosure of which could reasonably be expected to cause **damage** to national security.

For example, if we reveal information about our emergency defense plans to someone who doesn't need to know, it could harm our nation's defense.

<u>Unclassified</u> information is also official information, but it doesn't need the same safeguards as classified information. However, it may have certain restrictions against its release to unauthorized persons.

Some unclassified information is controlled by marking it "FOR OFFICIAL USE ONLY."

a. **FOR OFFICIAL USE ONLY (FOUO).** This is information that hasn't been given a security classification, but which should be publicly withheld for one or more reasons. For example, although not required to be marked FOUO, your personnel records are considered to be FOUO.

b. **National Security-Related Information.** Some unclassified information concerning national defense or US foreign relations is of possible intelligence value. When added to other unclassified information, it gives an insight into classified plans, programs, operations, or activities and becomes of intelligence value. For example, the number of fighter aircraft on the flightline is unclassified, but that information could be of value to the enemy.

Historically, OPSEC emerged during the Vietnam conflict. In Southeast Asia, the enemy had advanced knowledge of our operations which greatly reduced our effectiveness against them. To correct this problem, the Joint Chiefs of Staff (JCS) issued a Secretarial Memorandum initiating an operations security program armed-forces wide. The Pacific Air Force's program was code-named "Purple Dragon." The Purple Dragon program denied the enemy vital information and had an immediate impact on the effectiveness of our combat operations.

Indeed, our adversaries are able to obtain a significant amount of intelligence through human sources. They befriend us, seeking information about our military forces as well as about scientific or technological advances. If any foreign nationals or others seek information or material from you, even if it may seem insignificant, report it immediately to your supervisor, security manager, commander, or OSI.

We have the privilege of living in a great nation. To preserve the privileges and freedoms we enjoy, we must be constantly aware of the forces around us who would like to deprive us of our freedoms to further their own political and individual goals. To keep abreast of current programs and threats, the DoD has directed commanders to implement active OPSEC education programs. You must realize it's not only the military member or the DoD civilian who's targeted for information, but it can also be the family, too. Remember, the bad guy doesn't run around in the black trench coat with the upturned collar!

c. **Critical Information.** Information about friendly (US, allied or coalition) activities, intentions, capabilities or limitations that an adversary needs in order to gain a military, political, diplomatic or technological advantage are known as critical information. These are things that are so familiar to the average military member that they don’t think of them as being important. Some examples of critical information include but are not limited to exercise schedules, VIP visits, flight plans or increased working hours.

Communications Security (COMSEC)

COMSEC is the protection resulting from all measures designed to deny unauthorized persons information of value, which might be derived from analysis of telecommunications. It can be achieved only through effective defensive and preventive measures against thefts, espionage, observation, interception, traffic analysis, cryptoanalysis, deception, and other methods, which intelligence services employ.

The principle of COMSEC, defining the information which should be revealed, is simply this, "IF IT'S CLASSIFIED, OR DEALS WITH A CLASSIFIED PROJECT OR MISSION, OR CONTAINS INFORMATION ABOUT OUR CAPABILITIES, STRATEGY, PLANS, OR LIMITATIONS, GIVE IT ONLY TO THOSE WHO HAVE A DEFINITE NEED-TO-KNOW AND WHO HAVE THE PROPER SECURITY CLEARANCE BY A SECURE COMMUNICATIONS MEDIA."

Emission Security (EMSEC)

The Air Force Emission Security Program defines Emission Security (EMSEC) as the protection resulting from all measures taken to deny unauthorized access to information of value, which may be derived from intercept and analysis of compromising emanations. These emanations are usually electromagnetic or acoustic in nature. The term “TEMPEST” is used as a synonym for “compromising emanations.”

How do compromising emanations reach the enemy? They may travel through the air as radio waves (radiated signals) or through wires, pipes or other electrical conductors leaving an equipment area (conducted signals). The more power used in a device, the stronger its emanations, and the further they can travel long distances over wires. Telephones are particularly great emission security hazards since conducted signals near the telephone can be sent out as a signal on the line, and travel almost anywhere in the world. Proper grounding and distance from equipment that processes classified information are the most common means of preventing compromising emanations.

Remember, any knowledge about specific emission security hazards may alert enemy agents to possible sources of classified information. Don't tell anyone about a specific Emission Security hazard unless that person has a need-to-know and is cleared for the information.

Computer Security (COMPUSEC)

The broad, multi-disciplined area known as computer security encompasses all computers, from single-chip systems to large mainframes. It covers all applications including embedded computers, automated information systems, word processors, memory typewriters, and even memory calculators that have other than mathematical functions. It also includes hardware, software, operating systems, applications software, and firmware. The primary objective of the COMPUSEC program is to protect the privacy, availability, and integrity of systems and the information they process. The hardware, software, and information are protected according to the degree of data, sensitivity, criticality to mission, threats and vulnerabilities of the system, and an economic assessment of protective measures. Threats can be either human (intentional or unintentional), structural (facility or system), or natural. Several security disciplines, including physical, information, personnel, EMSEC, communications, and operations security, are integral parts of COMPUSEC. Take proper care when using computers as most violations occur through user carelessness.

Here are some additional requirements and conditions you should consider as part of your COMPUSEC responsibility:

a. Use your computer resources for official business only. The commander may grant use of these resources for educational purposes if such use benefits the Air Force (i.e., professional military education).

b. Protect your USERID/password.

c. Protect operating and application system software in accordance with copyright laws. Obtain software only through Air Force channels, never from non-Air Force bulletin boards, public domain software, or shareware.

d. Protect the computer environment by keeping it clean, and don't permit smoking, eating, or drinking in the computer area.

Misuse of system resources violates public trust placed on military and civilian government employees. It may also cause additional costs by denying the resources to authorized users. Military members may be prosecuted for these types of misuse violations under the UCMJ, Article 92, Failure to Obey an Order or Regulation.

Protection of the President

In the relatively short history of the United States, we've lost presidents Lincoln, Garfield, McKinley, and Kennedy to assassins. We've also had assassination attempts on seven former presidents.

You and I could prevent another President from losing his/her life; others like us may have already done so. You've all read newspaper accounts of persons being arrested by the United States Secret Service for making threats on the life of the president. These arrests were made based on information from someone who heard an individual make such remarks as "I'm going to kill that so-and-so," or "He's responsible for our troubles and I'm going to fix his wagon."

AFI 71-101V2, Protection of the President, states you must report such threats to your commander, the Security Forces, or the AFOSI. Under AFI 71-101V2, "President" refers to those present and past, government heads of state, and others.

Bibliography:

1. AFI 75-105, Counterintelligence Awareness and Briefing Program. Washington DC: Department of Air Force, 1 Apr 87. (Base Pubs Library)
2. AFI 31-401, Information Security Program Management, Washington DC: Department of the Air Force, 1 Jan 99.
3. AFI 31-501, Personnel Security Program Management, Washington DC: Department of the Air Force, 2 May 94.
4. AFI 10-1101, Operations Security, Washington DC: Department of the Air Force, 1 May 97.